

AO 106 (Rev. 04/010) Application for Search Warrant

AUTHORIZED AND APPROVED/DATE: /S Bow Bottomly 5/18/2021

amly
5/18/21

UNITED STATES DISTRICT COURT

WESTERN

for the
DISTRICT OF

OKLAHOMA

In the Matter of the Search of)
 (Briefly describe the property to be search)
 Or identify the person by name and address)
 Premises known as)
 3841 SE 54th)
 Oklahoma City, OK)

Case No: M-21-302-AMG

APPLICATION FOR SEARCH WARRANT

I, David A. Garrison, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property (*identify the person or describe property to be searched and give its location*):

See Attachment A, which is attached and incorporated by reference.

Located in the Western District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment B, which is attached and incorporated by reference

The basis for the search under Fed. R. Crim.P. 41(c) is (*check one or more*):

- ☒ evidence of the crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Title 18, U.S.C., § 2252A(a)(2)(A)

Offense Description

Attempted receipt of child pornography

Title 18, U.S.C., § 2252A(a)(5)(B)

Possession of child pornography

Title 18 U.S.C. § 2422(b)

Persuading or coercing a minor to engage in sexual activity

The application is based on these facts:

See attached Affidavit of Special Agent David A. Garrison, FBI, which is incorporated by reference herein.

☒ Continued on the attached sheet(s).

☐ Delayed notice of [No. of Days] days (*give exact ending date if more than 30 days*) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s)



Applicant's signature

David A. Garrison
Special Agent
FBI

Sworn to before me and signed in my presence.

Date: 5/18/21

City and State: Oklahoma City, Oklahoma

Printed name and title


Judge's signature

AMANDA M. GREEN, U.S. Magistrate Judge

Printed name and title

**THE UNITED STATES DISTRICT COURT FOR THE WESTERN
DISTRICT OF OKLAHOMA**

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, David A. Garrison, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent (SA) with the Federal Bureau of Investigation (FBI) since June 2005, and I am currently assigned to the Oklahoma City Field Office. Since joining the FBI, I have been involved in investigations of child exploitation matters and computer crimes against children. I currently investigate violations of federal law involving the exploitation of children. I have gained expertise in the conduct of such investigations through training in seminars, classes, and everyday work related to conducting these types of investigations in my current role as an SA with the FBI.

2. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. I am investigating the online activities of Greg Allen Henke ("HENKE"), who resides in 3841 SE 54th, Oklahoma City, OK 73135 (hereinafter referred to as the PREMISES). There is probable cause to believe that HENKE has attempted to receive and possessed child pornography, in violation of 18 U.S.C. §§ 2252 and 2252A and committed the crime of coercion and enticement of a minor, in violation of 18 U.S.C. § 2422(b).

4. This affidavit is submitted in support of an application for a search warrant for the location specifically described in Attachment A of this Affidavit: the residence of Greg Allen HENKE, 3841 SE 54th, Oklahoma City, OK 73135 (the "SUBJECT PREMISES"), which includes the entire house, curtilage, appurtenances, outbuildings, vehicles parked thereon, and any person present for property that constitutes: evidence of the commission of a criminal offense; contraband, the fruits of crime, and things otherwise criminally possessed; and property designed and intended for use, and which has been used as a means of committing criminal offenses, namely, the violations Title 18, United States Code, Sections 2252A (attempted receipt and possession of child pornography) and 2422(b) (coercion and enticement of a minor, which items are more specifically described in Attachment B of this Affidavit.

4. The statements in this Affidavit are based on my own investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A and 18 U.S.C. §§ 2422 are presently located within the SUBJECT PREMISES.

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that

resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

c. "Child Pornography" includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

d. "Computer" refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." *See* 18 U.S.C. § 1030(e)(1).

e. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not

limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

f. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alphanumeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

h. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

i. “Minor” means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).

j. “Sexually explicit conduct” applies to visual depictions that involve the use of a minor, *see* 18 U.S.C. § 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, *see* 18 U.S.C. § 2256(8)(C). In those contexts, the term refers to actual or simulated (a) sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).

k. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

l. The terms “records,” “documents,” and “materials” include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators,

electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

m. A “storage medium” or “storage device” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, “thumb,” “jump,” or “flash” drives, CD-ROMs, and other magnetic or optical media.

n. A “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

6. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed.

7. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

8. Child pornographers can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another

computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to millions of computers around the world.

9. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

10. The Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

11. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. These online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

12. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's

favorite websites in “bookmarked” files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user’s Internet activities generally leave traces in a computer’s web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data. Likewise, devices such as cellular telephones, tablets, and e-readers are also capable of electronic storage as computers.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

13. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components or seize most or all computer items (computer hardware, computer software, and computer-related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

- a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to
-

determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

14. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

15. Furthermore, I know that smart cell phones (a type of “computer,” as again, broadly defined in 18 U.S.C. § 1030(e)) can typically “sync” with a traditional desktop or laptop computer. The purpose of syncing a smart phone to a traditional computer is to back up data that is stored on the phone so that it is not permanently lost if the portable smart phone is lost or damaged. Also, smart phone users may move files off the smart phone and onto a computer to free up storage space on the smart phone. Similarly, computer (e.g., desktop computers, smart phones, etc.) users may move files off of one computer onto another computer or digital file storage devices such as a thumb drive, a DVD, an external hard drive to free up space on the computer. For this reason, I am seeking authorization to seize all computers and digital file storage devices at the SUBJECT PREMISES—not any particular computer. Finally, I know that many modern smart cell phones, including Apple iPhones and Samsung-brand phones, can be encrypted by the user using his finger and/or thumbprints to lock and unlock the device. Without the user's prints, the devices are difficult, if not impossible, for law enforcement personnel to unlock. Accordingly, I am requesting that, to the extent law enforcement seizes any smart cell phones or other computers described in Attachment B during a search of the SUBJECT PREMISES (described in Attachment A), and if such device(s) features such encryption, then law enforcement may, while executing the search warrant at the SUBJECT PREMISES, depress the owner's finger and/or thumbprints onto any such encryption feature to attempt to unlock the device.

BACKGROUND OF THE INVESTIGATION

13. In late March or early April of 2021, HENKE, utilizing an instant messaging Internet and phone application called Wickr, with the username, "jimdarling169", initiated a chat dialogue with a Confidential Human Source (CHS). Once HENKE expressed a sexual interest in minors, the CHS informed HENKE to contact the CHS's "uncle" who had control over the minors within the family.

14. The OCE began Wickr chatting with HENKE on April 5, 2021. HENKE continued to discuss his sexual attraction to minors and on April 10 expressed his favorite age range, "I'm ok with 5 and up to 13 or 14 but 6 to 10 is perfect." He also expressed how, "I'm bi...so I like boys and girls." Later that same day, HENKE wished, "I could see what they look like...your descriptions sound great...but I understand and respect your rules". The OCE had explained to HENKE how and why he did not share certain types of pictures of the referenced minors. HENKE went to describe in detail the kind of sexual activity he wished to engage in with the minors.

15. On May 1-2, 2021, after about a week and a half of no contact, HENKE reached out to the OCE again, via Wickr, and asked the OCE if he was still interested in arranging a meeting with the minors and added, "I am definitely still interested." On May 6, 2021, HENKE requested, "If you have any other pics of the kids...especially any with less clothes that you could send, then I could then send some pics of my niece that I used to enjoy before the pandemic came around." In earlier chats, HENKE described how he had a nine year old niece who he had babysat since she was five and enjoyed both looking at and touching her. HENKE went on to explain the pictures of his niece showed "other areas."

16. Later that day, HENKE added, "If you have pics of the kids, less clothes the better, then that would show that this is in fact 100% real and not something I need to worry about getting arrested, then I would send pics of my niece too." HENKE continued, ""You don't have to send any pics man.....I just thought that if you were sending explicit pics of the kids then that's proof your not a cop, and then I could send some of my niece."

17. On May 10, 2021, during an exchange leading up to the scheduled meet on May 13, 2021, in response to pictures sent by the OCE, HENKE said, "I've got naughtier pics I am willing to share, do u?" Later that day, HENKE added, "I want this as much as you. Maybe more...lol and I'm willing to share pics too." In response to the OCE not wanting to share pictures of his minors, HENKE replied, "What if you shared pics that were not them first...naughty pics from the internet. You have any of those first? Like I said, it's about feeling like getting stuff from someone that I know a cop wouldn't be able to send I can respect that, I understand the pics of them response...like I said what about other young pics from the internet?"

18. In response to the OCE being unwilling to share pictures of that nature, HENKE replied, "Dude...I understand, I want to be a part of this, I want it to become something just like you, And I have a collection I could share." After expressing more apprehension about the OCE being a cop and getting arrested, HENKE continued, "I am willing, I will share my nieces pics, I will share my collection." Still trying to convince the OCE to send explicit pictures of his minors, HENKE continued, "What if I send a naughtier pic of my niece and set the Wickr timer to a short time. So you can see it but then it disappears. Would you send one of the kids."

19. Later that day, the OCE sent HENKE a couple of links which directed him to a Mega online storage site containing two fake video files labeled as child pornography: "Jenny preteen teen fucked.mov" and "Jenny blow tits child.mov." HENKE reported accessing the links but neither video would play.

20. The nature of the chats between the OCE and HENKE progressed to HENKE choosing Thursday, May 13, 2021 at 11:00 a.m. to meet with the OCE and his children in order for HENKE to engage in sexual activities with the children. The OCE suggested that HENKE bring a gift for the children to help break the ice with them. The OCE sent a picture of a white Kid Connection Walking Unicorn toy that could be purchased at Walmart. Additionally, HENKE and the OCE agreed that the OCE would show HENKE the child pornography he had tried to send him earlier to prove the OCE was not law enforcement.

21. The OCE chose the Oyo Hotel on South I35 Service Road as the location for the sexual encounter and arranged with HENKE to meet there on May 13 at 11:00 a.m.

22. Upon arrival at the hotel, the OCE was contacted by HENKE who expressed concern over meeting at the hotel due to a couple of security guards he observed there when he drove around the parking lot earlier that morning. He suggested they meet at a nearby restaurant or similar location then go to his house.

23. The OCE suggested to Henke that they meet at the parking lot of the Crossroads Mall near I240 and I35. Henke eventually agreed. At approximately 10:30 a.m., HENKE arrived in a Ford truck. Upon his arrival, the OCE walked to HENKE's vehicle and asked HENKE if he was "Jim." HENKE responded yes and shortly thereafter

was arrested by agents from the Oklahoma City Field Office of the FBI. Incident to his arrest, while conducting a safety search of areas of the truck within HENKE's reach, a bag was observed containing children's toys. One of the toys was the referenced white Walking Unicorn. Additionally, incident to his arrest, HENKE's cell phone, a Samsung Galaxy S10 SM-G973U, FCC ID-A3LSMG973U, IMEI-352330100495543, was seized from the HENKE's vehicle.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

24. The following indicates characteristics of child pornography collectors that this Affiant has learned through training, working multiple investigations involving child pornography, and from other law enforcement officers with a background in child pornography investigations:

a. The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

b. The majority of individuals who collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children.

c. The majority of individuals who collect child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P, e-mail, e-mail groups, bulletin boards, IRC, newsgroups, instant messaging, and other similar vehicles.

d. The majority of individuals who collect child pornography maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings, and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

e. The majority of individuals who collect child pornography often collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

f. The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. They almost

always maintain their collections in the privacy and security of their homes or other secure location.

g. In light of the aforementioned, including the facts that demonstrate HENKE may possess child pornography, attempted to possess child pornography, and that he coerced and entice a minor to engage in sexual activity, I think (based on my training and experience) that it is highly probable that HENKE is a child pornography collector.

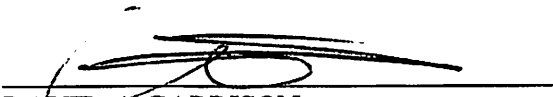
h. Based on the evidence in this investigation, I believe that HENKE, residing at the SUBJECT PREMISES, likely displays characteristics common to individuals who distribute, receive, possess, and/or access with intent to view child pornography.

CONCLUSION

25. Based on the aforementioned factual information, I submit that there is probable cause to believe that Greg HENKE has committed the crime of possession, and attempted receipt of child pornography, in violation of Title 18 U.S.C. §§ 2252 and 2252A; and committed the crime of coercion and enticement of a minor, in violation of 18 U.S.C. § 2422(b). Additionally, I submit that there is probable cause to believe that evidence of those criminal offenses is located within the SUBJECT PREMISES, and that this evidence, listed in Attachment B to this Affidavit, which is incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses.

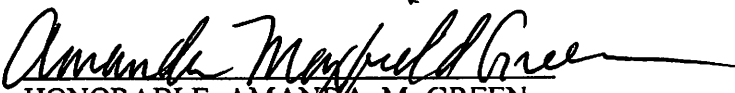
26. I respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

27. I am aware that the recovery of data by a computer forensic analyst takes significant time. Much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the “return” inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.



DAVID A GARRISON
SPECIAL AGENT
FEDERAL BUREAU OF INVESTIGATION

Sworn and subscribed before me this 18th day of May, 2021.



HONORABLE AMANDA M. GREEN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

ITEMS TO BE SEARCHED

1. 3841 SE 54th Street, Oklahoma City, Oklahoma is a single story residence located on the northwest corner of SE 54th Street and S Huddleston Street in Oklahoma City, Oklahoma.

Images of the SUBJECT PREMISES:





This warrant authorizes the forensic examination of the SUBJECT PREMISES for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

1. Computer(s), as broadly defined in 18 U.S.C. § 1030(e) and all other digital file storage devices, including (but not limited to) desktop computers, smart phones, e-readers, tablets, thumb drives, SD cards, DVDs, compact discs, and external hard drives; all computer hardware, computer software; computer related devices and documentation; computer passwords and data security devices; videotapes; video recording devices; video recording players; and video display monitors that may be, or are used to visually depict child pornography or child erotica, display or access information pertaining to a sexual interest in child pornography, display or access information pertaining to sexual activity with children, or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

4. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.

5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of the computer or by other means for the purpose of distributing or receiving child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat

logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.

9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

12. Any and all cameras, film, videotapes or other photographic equipment capable of storing images or videos of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.

13. Any and all visual depictions of minors.

14. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including

by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

15. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

16. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

17. Any and all equipment associated with routers, modems, and network equipment used to connect computers to the Internet.

18. If a smart cell phone or other computer, as described herein, is found that requires access by using a finger or thumbprint to unlock the device, then, while executing the search warrant at the SUBJECT PREMISES, a law enforcement officer may press the finger or thumbprint of any occupant of the SUBJECT PREMISES onto the device to try to unlock it.

19. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the offense of coercion enticement of a minor to engage in sexual activity, in violation of 18 U.S.C. § 2422(b).